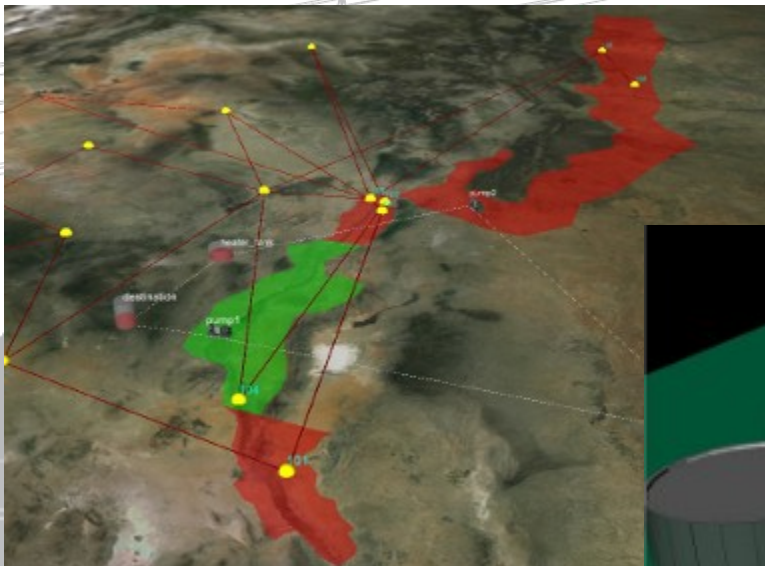# Virtual Control System Environment

Control System Design & Analysis Tool

The Virtual Control System Environment (VCSE) is a modeling and simulation environment that bridges the gap between control system models and process simulation. Tools and techniques exist for simulating and emulating control system field devices, but results from the security analysis these tools currently support are limited because the physical processes being controlled are not included. Leveraging Sandia's proven Umbra modeling environment, the VCSE intertwines the device and process simulations to provide an integrated system capable of representing realistic responses in the physical process as events occur in the control system and vice versa.

Modeling & Simulation

The VCSE is comprised of simulated control system devices, such as remote terminal units (RTUs), programmable logic controllers (PLCs) and protection relays, and simulated processes, such as electric power transmission systems, refinery processes, and pipelines. The simulated control system devices are capable of communicating over Internet Protocol (IP) networks using standard Supervisory Control and Data Acquisition (SCADA) protocols like Modbus and DNP3. The VCSE also includes support for hardware-in-the-loop, wherein real field devices under study (i.e. a specific model of PLC) can be connected to and interact with the physical process being simulated.

Benefits

The VCSE provides a means for creating large-scale control system test environments suitable for cyber security experiments. Leveraging modeling and simulation, the test environments can be scripted to suite each experiment as necessary, are repeatable, and are much cheaper to construct than real or even lab-scale test environments. The use of standards-based SCADA protocols in the simulated field devices also means 3rd party ICS and cyber security testing applications can still be used, and supports the use of simulated and emulated network environments as well.

Security Analysis

The VCSE provides an analysis capability that supports assessing and improving the cyber security of control systems used in the energy sector as described by The Roadmap to Secure Control Systems in the Energy Sector. The VCSE provides an environment where hardware and software upgrades and new mitigations can be evaluated before installation in an operational environment.

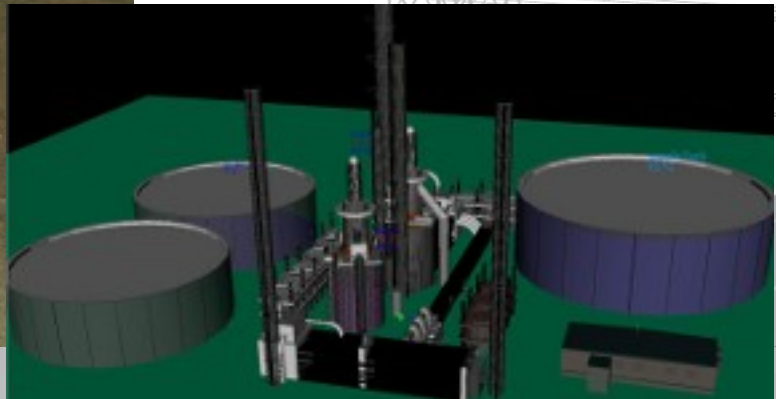*For more information, contact:*
Sandia National Laboratories
Bryan T. Richardson
P.O. Box 5800 MS 0671
Albuquerque, NM 87185-0671
Phone: (505) 845-2386
Email: btricha@sandia.gov